



(51) 国際特許分類6
G09C 1/00, H04L 9/06

A1

(11) 国際公開番号

WO99/00783

(43) 国際公開日

1999年1月7日(07.01.99)

(21) 国際出願番号

PCT/JP98/02915

(22) 国際出願日

1998年6月30日(30.06.98)

(30) 優先権データ

特願平9/173672

1997年6月30日(30.06.97)

JP

(71) 出願人 (米国を除くすべての指定国について)

日本電信電話株式会社(NIPPON TELEGRAPH AND
TELEPHONE CORPORATION)[JP/JP]

〒163-8019 東京都新宿区西新宿三丁目19番2号 Tokyo, (JP)

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ)

神田雅透(KANDA, Masayuki)[JP/JP]

高嶋洋一(TAKASHIMA, Youichi)[JP/JP]

〒163-1419 東京都新宿区西新宿3丁目20-2

日本電信電話株式会社内 Tokyo, (JP)

青木克彦(AOKI, Katsuhiko)[JP/JP]

〒107-0062 東京都港区南青山5-11-5 Tokyo, (JP)

松本 勉(MATSUMOTO, Tsutomu)[JP/JP]

〒227-0048 神奈川県横浜市青葉区柿の木台13-45

Kanagawa, (JP)

(74) 代理人

弁理士 草野 卓, 外(KUSANO, Takashi et al.)

〒160-0022 東京都新宿区新宿四丁目2番21号 相模ビル
Tokyo, (JP)(81) 指定国 CA, US, 欧州特許 (AT, BE, CH, CY, DE, DK,
ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

添付公開書類

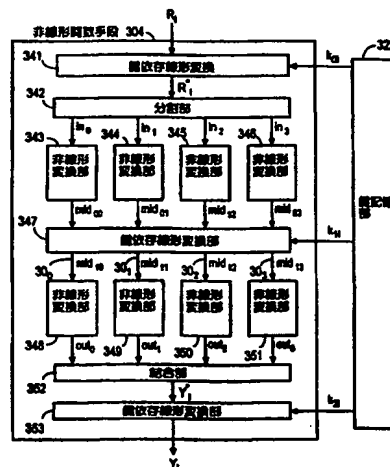
国際調査報告書

(54) Title: CIPHERING APPARATUS

(54) 発明の名称 暗号装置

(57) Abstract

A ciphering apparatus of common key type, wherein a plurality of rounding units are connected in cascade, the i -th rounding unit is fed with input data L_i , R_i , the input data R_i are subjected to nonlinear transformation by a nonlinear function unit depending upon the key data, the exclusive-OR output of the output of the nonlinear function unit and the input data L_i is outputted as data R_{i+1} to the $(i+1)$ -th rounding unit, and the input data R_i are outputted as data L_{i+1} to the $(i+1)$ -th rounding unit. The nonlinear function unit includes: a key-dependent linear transforming unit for subjecting the input R_i to key-dependent linear transformation; a dividing unit for dividing the output into four data in_0 , in_1 , in_2 and in_3 ; first nonlinear transforming units for subjecting the divided data to nonlinear transformation to output data mid_{00} , mid_{01} , mid_{02} and mid_{03} ; a key-dependent linear transforming unit for correlating these transformed outputs to each other and subjecting them to linear transformation based upon the key data to output data mid_{10} , mid_{11} , mid_{12} and mid_{13} ; second nonlinear transforming units for subjecting the transformed outputs to nonlinear transformation to output data out_0 , out_1 , out_2 and out_3 ; and a coupling unit for coupling the transformed outputs to output data Y .



- | | |
|------------------------------------------------|------------------------------------------------|
| 304 ... Nonlinear function means | 348 ... Nonlinear transforming unit |
| 341 ... Key-dependent linear transformation | 349 ... Nonlinear transforming unit |
| 342 ... Dividing unit | 350 ... Nonlinear transforming unit |
| 343 ... Nonlinear transforming unit | 351 ... Nonlinear transforming unit |
| 344 ... Nonlinear transforming unit | 352 ... Coupling unit |
| 345 ... Nonlinear transforming unit | 353 ... Key-dependent linear transforming unit |
| 346 ... Nonlinear transforming unit | 322 ... Key storage unit |
| 347 ... Key-dependent linear transforming unit | |

(57)要約

共通鍵型の暗号装置において、複数段のラウンド処理部が従属接続して設けられ、各 i 段のラウンド処理部は入力データ L_i , R_i が与えられ、入力データ R_i を非線形関数部により鍵データに応じて非線形変換し、その出力と、入力データ L_i との排他的論理和出力を次段に与えるデータ R_{i+1} として出力し、入力データ R_i を次段に与えるデータ L_{i+1} として出力し、各段の非線形関数部は、入力 R_i を鍵依存線形変換する鍵依存線形変換部と、その出力を 4 つのデータ ino , in_1 , in_2 , in_3 に分割する分割部と、これら分割データをそれぞれ非線形変換してデータ mid_0 , mid_{01} , mid_{02} , mid_{03} を出力する第 1 の非線形変換部と、これら変換出力を互いに関連づけると共に、鍵データに基づいてそれぞれ線形変換してデータ mid_{10} , mid_{11} , mid_{12} , mid_{13} を出力する鍵依存線形変換部と、それらの変換出力をそれぞれ非線形変換し、データ out_0 , out_1 , out_2 , out_3 を出力する第 2 の非線形変換部と、それらの変換出力を結合しデータ Y を出力する結合部とを含む。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AL	アルバニア	FI	フィンランド	LK	スリ・ランカ	SI	スロヴェニア
AM	アルメニア	FR	フランス	LR	リベリア	SK	スロヴァキア
AT	オーストリア	GA	ガボン	LS	レソト	SL	シエラ・レオネ
AU	オーストラリア	GB	英国	LT	リトアニア	SN	セネガル
AZ	アゼルバイジャン	GD	グレナダ	LU	ルクセンブルグ	SZ	スワジランド
BA	ボスニア・ヘルツェゴビナ	GE	グルジア	LV	ラトヴィア	TD	チャード
BB	バルバドス	GH	ガーナ	MC	モナコ	TG	トーゴ
BE	ベルギー	GM	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BF	ブルキナ・ファソ	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BG	ブルガリア	GW	ギニア・ビサウ	MK	マケドニア旧ユーゴスラヴィア	TR	トルコ
BJ	ベナン	GR	ギリシャ		共和国	TT	トリニダード・トバゴ
BR	ブラジル	HR	クロアチア	ML	マリ	UA	ウクライナ
BY	ベラルーシ	HU	ハンガリー	MN	モンゴル	UG	ウガンダ
CA	カナダ	ID	インドネシア	MR	モーリタニア	US	米国
CF	中央アフリカ	IE	アイルランド	MW	マラウイ	UZ	ウズベキスタン
CG	コンゴ	IL	イスラエル	MX	メキシコ	VN	ヴィエトナム
CH	スイス	IN	インド	NE	ニジェール	YU	ユーゴスラビア
CI	コートジボアール	IS	アイスランド	NL	オランダ	ZW	ジンバブエ
CM	カメルーン	IT	イタリア	NO	ノールウェー		
CN	中国	JP	日本	NZ	ニュー・ジーランド		
CU	キューバ	KE	ケニア	PL	ポーランド		
CY	キプロス	KG	キルギスタン	PT	ポルトガル		
CZ	チェッコ	KP	北朝鮮	RO	ルーマニア		
DE	ドイツ	KR	韓国	RU	ロシア		
DK	デンマーク	KZ	カザフスタン	SD	スーダン		
EE	エストニア	LC	セントルシア	SE	スウェーデン		
ES	スペイン	LI	リヒテンシュタイン	SG	シンガポール		

明細書

暗号装置

技術分野

この発明は、データの通信または保持において、データを秘匿するための暗号化装置、特に、秘密鍵の制御のもとでデータをブロック単位で暗号化または復号を行う共通鍵暗号方式による暗号化装置に関するものである。

従来の技術

データを秘匿するための暗号化装置に含まれる代表的な共通鍵暗号方式には、米国連邦標準暗号であるDES (Data Encryption Standard) 暗号がある。

図1は、DES暗号の機能構成を示す。DES暗号では、56ビットの秘密鍵を用い、64ビットのデータブロック単位に暗号化または復号を行う。図1において、暗号化処理は、平文Pの64ビットを初期変転部11において初期転値で変換した後、32ビットごとのブロックデータ L_0 , R_0 に分割される。ブロックデータ R_0 は図2に第*i*段ラウンド処理部14_{*i*} ($i=0, 1, \dots, 15$) のものとして示す関数演算部 (ラウンド関数と呼ばれている) 12へ入力され、48ビットの拡大鍵 k_0 の制御のもとに $f(R_0, k_0)$ に変換される。この変換データ $f(R_0, k_0)$ とブロックデータ L_0 との排他的論理和をXOR回路13でとり、その出力とブロックデータ R_0 とを入れ替えて、次のブロックデータ L_1 , R_1 とする。即ち、

$$\begin{aligned} R_1 &= L_0 \oplus f(R_0, k_0) \\ L_1 &= R_0 \end{aligned} \quad (1)$$

である。

このように2つのブロックデータ L_0 , R_0 を入力として演算部12と排他的論理和回路13とデータの入れ替え (スワップ) とにより L_1 , R_1 を出力する第0段ラウンド処理部14₀が構成され、同じようなラウンド処理部14₁ ~ 14₁₅が縦続的に設けられる。第*i*段ラウンド処理部14_{*i*}による処理を第*i*段のラウンド処理と呼ぶことにする。ただし、 $i=0, \dots, 15$ である。つまり各ラウンド処理部14_{*i*} ($0 \leq i < 15$) では、

$$R_{i+1} = L_i \oplus f(R_i, k_i)$$

$$L_{i+1} = R_i \quad (2)$$

の処理が行われ、最後に R_{16} , L_{16} を統合して 64 ビットにした後、最終転値部 15 において最終転値で変換して暗号文 64 ビットを出力する。復号処理においては、関数 f に入力する拡大鍵 $k_0, k_1, \dots, k_{14}, k_{15}$ の順序だけを逆転させて、 $k_{15}, k_{14}, \dots, k_1, k_0$ の順に入力するようにする点を除けば、暗号化処理と同じ手順で実行できる。その場合、最終段ラウンド処理部 14₁₅ のスワップ出力 L_{16} , R_{16} を、図に示すように更にスワップするように構成することにより、復号処理において暗号文を初期転置 11 に入力して図 1 の処理を実行することにより、最終転置 15 の出力に平文がそのまま得られる。勿論、最終段ラウンド処理部 14₁₅ の出力をスワップしないで最終転置 15 にデータを与える構成としても全く同じである。なお、拡大鍵 $k_0, k_1, \dots, k_{14}, k_{15}$ は、暗号化処理とは別の拡大鍵生成ルーチン 16 で 56 ビットの秘密鍵が 48 ビットの拡大鍵 16 個の計 768 ビットに拡大されることによって生成される。

関数演算内部 12 の処理は、図 2 に示すように行われる。まず、32 ビットのブロックデータ R_i は拡大転値部 17 で 48 ビットデータ $E(R_i)$ に変換される。これに拡大鍵 k_i とで排他的論理和を XOR 回路 18 で取り、48 ビットデータ $E(R_i) \oplus k_i$ に変換した後、8 個の 6 ビットごとのサブブロックデータに分割する。この 8 個のサブブロックデータはそれぞれ異なる S-box $S_1 \sim S_8$ に入力され、各々が 4 ビットの出力を得る。なお、この S-box S_j ($j=1, \dots, 8$) は 6 ビットの入力データから 4 ビットの出力データに変換する非線形変換テーブルであり、DES 暗号の本質的な安全性を担っている部分である。S-box $S_1 \sim S_8$ の 8 つの出力データは、再び連結されて 32 ビットデータになった後、転置変換部 19 を経て、図 8 に示されるように、 L_i と排他的論理和される関数 f の出力 $f(R_i, k_i)$ となる。

次に、暗号解読法について述べる。DES 暗号を始めとする従来の共通鍵暗号方式についてはさまざまな方面から暗号解読が試みられており、そのなかでも、極めて効果的な解読法であるのが E. Biham 及び A. Shamir によって提案された差分解読法 (“Differential Cryptanalysis of DES-like Cryptosystems.” Proceedings of CRYPTO'90) と松井によって提案された線形解読法 (“DES 暗号

の線形解読法 (I), ” 1993 年暗号と情報セキュリティシンポジウム SCIS93-3C) である。

差分解読法は、2つのデータ X, X^* の差分を

$$\Delta X = X \oplus X^* \quad (3)$$

としたとき、解読者が入手している平文・暗号文の2組を以下の式に適用して、最終ラウンドにおける拡大鍵 k_{15} を求めることを目的としている。図1の暗号化処理において、既知の第1平文を入力したときの各ラウンド処理部14_iでの入力ブロックデータを L_i, R_i とし、既知の第2平文を入力したときの各ラウンド処理部14_iでの入力ブロックデータを L^*_i, R^*_i とする。これら第1及び第2平文が入力されたときの出力暗号文がそれぞれ既知であるとする。上記式(3)の定義により

$$\begin{aligned} \Delta L_i &= L_i \oplus L^*_i \\ \Delta R_i &= R_i \oplus R^*_i \end{aligned} \quad (4)$$

である。図1において、 $L_{15}=R_{14}, L^*_{15}=R^*_{14}, L_{16}=R_{15}, L^*_{16}=R^*_{15}$ なので、

$$\begin{aligned} R_{16} &= L_{15} \oplus f(R_{15}, k_{15}) \\ R^*_{16} &= L^*_{15} \oplus f(R^*_{15}, k_{15}) \end{aligned} \quad (5)$$

が成立し、これら2つの式の両辺の排他的論理和を取ると

$$\Delta R_{16} = \Delta L_{15} \oplus f(L_{16}, k_{15}) \oplus f(L_{16} \oplus \Delta L_{16}, k_{15}) \quad (6)$$

が得られ、その両辺と $\Delta R_{14} = \Delta L_{15}$ との排他的論理和を取ることにより次の式が得られる：

$$f(L_{16}, k_{15}) \oplus f((L_{16} \oplus \Delta L_{16}), k_{15}) = \Delta R_{16} \oplus \Delta R_{14} \quad (7)$$

このとき、 $L_{16}, \Delta L_{16}, \Delta R_{16}$ は暗号文から得られるデータであるので既知の情報である。このため、解読者が ΔR_{14} を正しく求めることができるならば、上式は k_{15} のみが未知定数となり、既知の平文・暗号文の組を用いて k_{15} に関する全数探索を行うことで、解読者は必ず正しい k_{15} を見つけたことができる。一方、 ΔR_{14} についてみてみると、この値は中間差分値であるため、一般には求めることが困難である。そこで、0ラウンド目から最終ラウンドの一つ前までのラウンド目までにおいて、各ラウンドが確率 p_i で

$$\Delta R_{i+1} = \Delta L_i \oplus \Delta \{f(\Delta R_i)\}$$

$$\Delta L_{i+1} = \Delta R_{i+1} \quad (8)$$

のように近似されたとおく。ここでのポイントは、ある ΔR_i が入力されたとき、拡大鍵 k_i の値に関わらず、確率 p_i で $\Delta \{f(\Delta R_i)\}$ を予測できるということにある。このように近似できるのは、 $\Delta \{f(\Delta R_i)\}$ に影響を与えるのが非線形な変換である S-box の部分だけであり、しかも S-box において、入力差分によっては差分出力の分布に極めて大きな偏りが生じるためである。例えば、S-box S_i では、入力差分 "110100" のとき、1/4 の確率で出力差分 "0010" に変換されるためである。そこで、各々の S-box が確率 $p_{i,j}$ で入力差分と出力差分との関係が予測できるとおき、これらを組み合わせることで各ラウンドの近似を求める。更に、各ラウンドでの近似を連結していくことで、 ΔR_{14} は確率 $P = \prod p_i$ で ΔL_0 , ΔR_0 (ΔL_0 , ΔR_0 は平文から得られるデータであるので既知の情報である) から求められることになる。なお、この確率 P が大きいほど、暗号解読が容易である。このようにして、拡大鍵 k_{15} が求められると、今度は 1 段少ない 15 段 DES 暗号とみなして、同様の手法で、拡大鍵 k_{14} を求めていくということを繰り返して、最終的に拡大鍵 k_0 まで求めていく。

Biham らによると、この解読法では、 2^{47} 組の選択された既知平文・暗号文の組があれば DES 暗号を解読できるとしている。

また、線形解読法は、以下の線形近似式を構成し、解読者が入手している平文・暗号文の組による最尤法を用いて拡大鍵を求めることを目的としている。

$$\begin{aligned} (L_0, R_0) \cdot \Gamma(L_0, R_0) \oplus (L_{16}, R_{16}) \cdot \Gamma(L_{16}, R_{16}) \\ = (k_0, k_1, \dots, k_{15}) \cdot \Gamma(k_0, k_1, \dots, k_{15}) \end{aligned} \quad (9)$$

ただし、 $\Gamma(X)$ は X の特定のビット位置を選択するベクトルを表し、マスク値という。

線形近似式の役割は、暗号アルゴリズム内部を線形表現で近似的に置き換え、平文・暗号文の組に関する部分と拡大鍵に関する部分とに分離することにある。つまり、平文・暗号文の組に関して、平文の特定のビット位置の値と暗号文の特定のビット位置の値との全ての排他的論理和が一定値となり、その値は拡大鍵の特定のビット位置の値の排他的論理和に等しくなることを表している。従って、解読者は

$$(L_0, R_0) \cdot \Gamma(L_0, R_0) \oplus (L_{16}, R_{16}) \cdot \Gamma(L_{16}, R_{16})$$

の情報から

$$(k_0, k_1, \dots, k_{15}) \cdot \Gamma(k_0, k_1, \dots, k_{15}) \quad (1 \text{ ビット})$$

の情報が得られるということになる。このとき、 (L_0, R_0) 、 (L_{16}, R_{16}) はそれぞれ平文・暗号文のデータであるので既知の情報である。このため、解読者が $\Gamma(L_0, R_0)$ 、 $\Gamma(L_{16}, R_{16})$ 、 $\Gamma(k_0, k_1, \dots, k_{15})$ を正しく求めることができるならば、 $(k_0, k_1, \dots, k_{15}) \cdot \Gamma(k_0, k_1, \dots, k_{15})$ (1 ビット)を求めることができる。

DES暗号では、非線形な変換が行われるのはS-box においてだけであり、従ってS-box についてのみ線形表現ができれば、容易に線形近似式が構成できる。そこで、各々のS-box S_i が確率 p_i で線形表現できるとおく。ここでのポイントは、S-box に対する入力マスク値が与えられたとき、確率 p_i でその出力マスク値を予測できるということにある。これは、非線形変換テーブルであるS-box において、入力マスク値によっては差分マスク値の分布に極めて大きな偏りが生じるためにおこる。例えば、S-box S_5 では、入力マスク値"010000"のとき、3/16の確率で出力マスク値"1111"が予測されるためである。これらS-box におけるマスク値を組み合わせることによって、各ラウンドが確率 p_i で入力マスク値と出力マスク値のあいだに線形近似することができ、各ラウンドでの線形近似を連結していくことで、 $\Gamma(L_0, R_0)$ 、 $\Gamma(L_{16}, R_{16})$ 、 $\Gamma(k_0, k_1, \dots, k_{15})$ は確率

$$P = 2^{n-1} \prod |p_i - 1/2| \quad (10)$$

で求められることになる。なお、この確率 P が大きいほど、暗号解読が容易である。

松井によると、この解読法で、 2^{43} 組の既知平文・暗号文の組を用いて、DES暗号の解読に成功している。

さて、上記の解読法に対抗するためには、確率 P が十分に小さくなればよい。このため、確率 P を小さくするための提案がさまざま行われており、なかでも従来の暗号方式において、もっとも簡単に安全性を高めるための方法がラウンド数を増やすことであった。例えば、DES暗号を3つつなげたTriple-DES暗号は、実質的にDESのラウンド数を16段から48段に増やした暗号方式であり、確

率 P は、DES 暗号よりもはるかに小さい。

しかし、上記の解読法に対抗するための対策として、ラウンド数を増加させることは、暗号装置の規模が大きくなり、データの処理量も増加することになる。例えば、ラウンド数を 3 倍に増やせば、暗号化処理量も 3 倍になる。つまり、現在の DES 暗号の暗号化速度は Pentium PC クラスで約 10Mbps であるため、Triple-DES 暗号ともなると約 3.5Mbps まで暗号化速度が低下する。一方で、ネットワークやコンピュータなどは年々高速化しており、暗号化装置もそれらの高速化に対応したものが望まれている。このため、従来の暗号装置では、それらの高速化の要求に対して、安全性と高速性を同時に満たすことはきわめて困難な状況になっている。

この発明の目的は、上記の点を鑑みなされたもので、ラウンド段数を増加させることなく安全性条件を満たすような暗号装置を提供することにある。

発明の開示

この発明では、特に非線形関数部において、非線形関数部の入力データに鍵記憶部に保持された鍵データに基づいて線形変換を行う鍵依存線形変換部と、この鍵依存線形変換部の出力データを複数個のビット列に分割する分割部と、これら分割された各ビット列に非線形変換をそれぞれ行う第 1 の非線形変換部と、その第 1 の非線形変換部の各々の出力ビット列間で線形変換を行う第 1 の線形変換部と、その第 1 の線形変換部の出力ビット列の一部またはすべてに非線形変換を行う第 2 の非線形変換部と、その第 2 の非線形変換部の出力ビット列をその非線形関数部の出力データに結合する結合部とを備えることを特徴とする。

更に安全性を向上させるには、上記結合部の出力データを上記非線形関数部の出力データに線形変換を行う第 2 の線形変換部を備えることを特徴とする。

また、上記第 1 の線形変換部または上記第 2 の線形変換部、もしくはその両方の部が、データの線形変換を行うときに、上記鍵記憶部に保持された鍵データに基づいて線形変換を行う鍵依存線形変換部であることを特徴とする。

この発明によれば、S-box における確率が $p_{i,j} \leq p_b < 1$ であるとき (p_b は S-box の最大差分又は線形確率)、各ラウンドを近似するときの確率は $p_{i,j} \leq p_b^2$ (ただし、差分解読法の場合は関数 f への入力差分が 0 でないとき、線形解読

法の場合は関数 f での出力マスク値が 0 でないとき) となることが保証される。また、関数 f が全単射 (入力が異なれば出力が必ず異なる) であるとき、暗号方式のラウンド数を $3m$ とすると、暗号方式としての確率は $P \leq p_b^{2m} \leq p_b^{4m}$ となる。一般に、暗号方式では $P < 2^{-64}$ であれば差分解読法や線形解読法に対して安全とされるため、 $m > -16 / \{\log_2(p_b)\}$ を満たせばよく、 $p_b \leq 2^{-4}$ であれば DES 暗号の 16 ラウンドよりも少ないラウンド数で安全性を確保できる。なお安全性の確率は m ラウンドの倍数ごとに変化する。

この発明によれば、差分解読法や線形解読法に対する安全性を比較的少ないラウンド数で確保できるため、安全性と低処理量を両立させた暗号装置を提供することが可能になる。

図面の簡単な説明

図 1 は従来の DES 暗号装置の機能構成を示す図。

図 2 は図 1 中の f 関数演算部 12 の具体的機能構成を示す図。

図 3 はこの発明の実施例 1 の機能構成を示す図。

図 4 は実施例 1 における非線形関数部 304 の詳細な機能構成例を示す図。

図 5 は図 4 中の鍵依存線形変換部 347 の具体例を示す図。

図 6 はこの発明の実施例 2 の機能構成を示す図。

図 7 A は実施例 2 における非線形関数部 304 の詳細な機能構成を示す図。

図 7 B はこの非線形関数部 304 における線形変換部 354 の具体例を示す図。

図 8 はこの発明の実施例 3 の機能構成を示す図。

図 9 は実施例 3 における非線形関数部 304 の詳細な機能構成を示す図。

発明を実施する最良の形態

実施例 1

以下、この発明の一実施例を図面を用いて説明する。

図 3 は、この発明の一実施例を示す暗号装置における、暗号化処理手順の機能構成を示したものである。この発明による暗号装置においても、入力データを 2 つのブロックデータ L_0 , R_0 に分割し、それらを順次ラウンド処理する n 段に従属

接続されたラウンド処理部 38₀～38_{n-1}が設けられ、各ラウンド処理部 38_i (i=0, 1, ..., n-1) は図 1 のラウンド関数部 12 に対応する非線形関数部 304 と、図 1 の XOR 回路 13 に対応する線形演算部 305 と、交換部 306 とから構成されている。

平文に相当する入力データ P を入力部 301 から暗号装置内に入力する。予め、鍵入力部 320 から入力されたデータに基づいて鍵データ生成部 321 により鍵データ

$$\{fk; k_{00}, k_{10}, k_{20}; k_{01}, k_{11}, k_{21}; \dots; k_{0(n-1)}, k_{1(n-1)}, k_{2(n-1)}; ek\}$$

が生成され、鍵記憶部 322 に保持される。入力平文データ P は鍵記憶部 322 に保持されている鍵データ f k による鍵依存初期線形変換部 302 で変換された後、初期分割部 303 で 2 つのブロックデータ L₀, R₀ に分割される。例えば 64 ビットのデータが 32 ビットずつのブロックデータ L₀, R₀ に分割される。ブロックデータ R₀ は、鍵記憶部 322 に保持されている鍵データ k₀₀, k₁₀, k₂₀ と共に第 0 段ラウンド処理部 38₀ の非線形関数部 304 に入力され、変換処理によりデータ Y₀ に変換される。データ Y₀ とブロックデータ L₀ は線形演算部 305 で演算されてデータ L₀^{*} に変換される。データ L₀^{*} とブロックデータ R₀ は交換部 306 でデータ位置の交換 (スワップ) が行われ、L₁=R₀, R₁=L₀^{*} とされ、L₁, R₁ が次の第 1 段ラウンド処理部 38₁ に入力される。

以下、第 i 段ラウンド処理部 38_i (i=1, ..., n-1) において、2 つの入力ブロックデータ L_i, R_i について上記と同様の処理を繰り返し行う。即ち、第 i 段ラウンド処理部 38_i においては、2 つのブロックデータ L_i, R_i のうちの、データ R_i は、鍵記憶部 322 に保持されている鍵データ k_{0i}, k_{1i}, k_{2i} と共に非線形関数部 304 に入力され、非線形関数部 304 で変換処理を受け、データ Y_i に変換される。データ Y_i とブロックデータ L_i は線形演算部 305 で演算されてデータ L_i^{*} に変換される。データ L_i^{*} とデータ R_i は交換部 306 でデータ位置の交換が行われ、L_{i+1}=R_i, R_{i+1}=L_i^{*} のように交換される。線形演算部 305 は例えば排他的論理和演算を行うものである。

暗号方式としての安全性を確保するための適切な繰り返し回数を n とすると、ラウンド処理部 38₀～38_{n-1} による繰り返し処理の結果、データ L_n, R_n が得られる。

このデータ L_n , R_n を最終結合部307 で1つのブロックデータに結合し、つまり例えば32ビットの各 L_n , R_n をビット結合して64ビットのデータとし、その後、鍵記憶部322 に保持されている鍵データ e_k を使って鍵依存最終線形変換部308 で変換し、出力部309 から暗号文として出力データ C を出力する。

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文 C から平文 P が得られる。例えば図3において入力データの代りに暗号文データを入力し、鍵データを図3とは逆に、 e_k , $k_{0(n-1)}$, $k_{1(n-1)}$, $k_{2(n-1)}$, \dots , k_{01} , k_{11} , k_{21} , k_{00} , k_{10} , k_{20} , f_k を順次与えればよい。

図4は、各ラウンド処理部38_i に使用されている非線形関数部304 の機能構成を示す。第 i 段ラウンド処理部38_i の入力ブロックデータ R_i は、鍵記憶部322 に保持されている鍵データ k_{0i} , k_{1i} , k_{2i} と共に非線形関数部304 への入力データとなる。ブロックデータ R_i は、鍵データ k_{0i} を使用した鍵依存線形変換部341 によりデータ R_i^* に線形変換される。データ R_i^* は分割部342 において例えば8ビットずつの4つのデータ in_0 , in_1 , in_2 , in_3 にビット分割される。4つのデータ in_0 , in_1 , in_2 , in_3 は、それぞれ非線形変換部343, 344, 345, 346において、データ mid_{00} , mid_{01} , mid_{02} , mid_{03} に非線形変換された後、鍵依存線形変換部347 に入力される。

鍵依存線形変換部347 は、図5に示すようにこの例ではそれぞれが少なくとも1つの排他的論理和を含む4つの処理系列30₀～30₃から構成され、これら処理系列はそれらの排他的論理和により互いに論理結合されている。各処理系列において他の処理系列のデータと線形演算（排他的論理和）を行うことにより、それぞれの処理系列において均質化されたデータを生成し、図5の例では更に鍵データ k_{1i} により線形処理される。即ち、データ mid_{00} , mid_{01} , mid_{02} , mid_{03} はそれぞれ処理系列30₀～30₃に入力され、処理系列30₁において入力データ mid_{00} と mid_{01} との排他的論理和がXOR31₁によりとられ、また処理系列30₂において入力データ mid_{02} と mid_{03} の排他的論理和がXOR31₂によりとられ、更にXOR31₁の出力とXOR31₂の出力の排他的論理和がXOR32₂によりとられる。XOR31₁の出力とXOR32₂の出力との排他的論理和がXOR33₁によりとられ、XOR33₁の出力と入力データ mid_{00} の排他的論理

和がXOR34₀によりとられ、XOR32₂の出力と入力データmid₀₃との排他的論理和がXOR34₃によりとられる。更に、XOR34₀, 33₁, 32₂, 34₃のそれぞれの出力と鍵データk₁₁₀, k₁₁₁, k₁₁₂, k₁₁₃との排他的論理和がXOR35₀～35₃によりとられて、それぞれmid₁₀, mid₁₁, mid₁₂, mid₁₃が出力される。つまり処理系列30₀～30₃の入力データmid₀₀, mid₀₁, mid₀₂, mid₀₃は相互に関連づけられた後、それぞれ鍵データk₁₁₀, k₁₁₁, k₁₁₂, k₁₁₃に依存した線形変換が行われる。論理式で示すと次式

$$\begin{aligned}
 \text{mid}_{10} &= \text{mid}_{00} \oplus \text{mid}_{02} \oplus \text{mid}_{03} \oplus k_{110} \\
 \text{mid}_{11} &= \text{mid}_{02} \oplus \text{mid}_{03} \oplus k_{111} \\
 \text{mid}_{12} &= \text{mid}_{00} \oplus \text{mid}_{01} \oplus \text{mid}_{02} \oplus \text{mid}_{03} \oplus k_{112} \\
 \text{mid}_{13} &= \text{mid}_{00} \oplus \text{mid}_{01} \oplus \text{mid}_{02} \oplus k_{113}
 \end{aligned} \tag{11}$$

の論理演算がなされる。これらの式から明らかなように、鍵依存線形変換部34の各処理系列の出力には少なくとも2つ以上の他の系列の入力データがこの例では排他的論理和の形で含まれており、従って、各系列の出力データには4つの入力データのうち、2つ以上の成分が含まれるように均質化されている。

これら出力データmid₁₀, mid₁₁, mid₁₂, mid₁₃は、それぞれの処理系列30₀～30₃に設けられた図4に示す非線形変換部348, 349, 350, 351において、データout₀, out₁, out₂, out₃に非線形変換された後、それぞれの処理系列の出力データとして結合部352に与えられ、一つのブロックデータY_i*に結合される。つまり、例えば4つの8ビットデータが1つの32ビットデータにビット結合される。このデータY_i*は、鍵依存線形変換部353において鍵データk₂₁によりデータY_iに線形変換され、非線形関数部304からの出力データY_iが生成される。非線形変換部343～346, 348～351のそれぞれは、例えばDES暗号における1つのS-boxと同様のもので、それぞれ入力データに応じた異った出力データを出力する例えばROMで構成される。

非線形変換部343～346は4つ並列に配置されており、それらの変換処理は相互に関連していないため、これらを並列実行することが可能であり、従って、これらの数が増加することによる処理時間の増大を並列処理により対処できる。非線形変換部348～351についても同様のことがいえる。

各段のラウンド処理部 381 を構成する線形演算部 305 (図 3)、線形変換部 341, 347, 353 (図 4) などの処理に要する時間は S-box と同様な非線形変換部 343~346, 348~351 等の処理に要する時間に比べてかなり短いので、暗号化処理に要する時間は使用される S-box 或いは非線形変換部の数にほぼ比例する。ところが、非線形変換部 348~351 については、鍵依存線形変換部 347 が前述のように複数の入力データを各出力に均質化して出力するため、鍵依存線形変換部 347 が、例えば図 5 のように特定の線形変換であることが予めわかっている場合には、非線形変換部 348~351 の何れか 1 つ或いは複数を省略し、対応するデータをそのまま結合部 352 に与えても、差分解読法及び線形解読法に対する安全性が低下しないようにすることができ、非線形変換を省略した分だけ暗号化処理量を削減できる。例えば、鍵依存線形変換部 347 が図 5 で表されているとき、非線形変換部 349, 350 を省略し、データ mid_{11} , mid_{12} をそのまま結合部 352 に入力しても差分解読法及び線形解読法に対する安全性は低下しない一方で、暗号化速度が約 33% 向上する。つまり鍵依存線形変換部 347 が予め決まっている場合は差分解読法、線形解読法に対しては非線形変換部 348~351 の 1 つ或いは複数はその存在が安全性に関係ない場合があり、その非線形変換は省略できる。

なお、図 3 において、鍵データ生成部 321 による鍵データ $\{fk, k_{00}, k_{10}, k_{20}, k_{01}, k_{11}, k_{21}, \dots, k_{0(n-1)}, k_{1(n-1)}, k_{2(n-1)}, ek\}$ の生成は図 1 の DES 暗号の拡大鍵生成アルゴリズム 16 と同様に行うことができる。

上記のように構成された暗号装置の場合、例えば、非線形変換部 343~346, 348~351 の各 1 つづつが差分解読法及び線形解読法に対して確率 $p_0 = 2^{-6}$ で近似表現できるように設計されているならば、各段のラウンド処理部 381 は非線形変換を必ず 2 回行うため、即ち、変換部 343~346 の処理と変換部 348~351 の処理を縦続して行うため、確率 $p_1 \leq 2^{-12}$ で近似表現することができ、暗号装置全体としてはラウンド数 n を $n = 3m$ として、確率 $P \leq 2^{-24m}$ で近似表現できることになる。ここで、例えば $m = 4$ (ラウンド数 12 段) とすると、 $P \leq 2^{-96}$ となり、DES のラウンド数 16 より少ないラウンド数で安全条件 $P < 2^{-64}$ を満たし、差分解読法及び線形解読法に対して十分安全な暗号装置となる。即ち、この発明は、従来のラウンド関数演算部 12 (図 1) 内において非線形変換を縦続して 2 回行

うように構成することにより、暗号解読に対し安全性を倍に高めることができる。

鍵依存初期線形変換部302、鍵依存最終線形変換部308、鍵依存線形変換部347, 353は鍵に依存する線形変換部であるため、差分解読法及び線形解読法以外の解読法に対しても十分な安全性を兼ね備え、もっとも安全性を重視した暗号装置である。

なお、この発明はこの例に特定されるだけでなく、例えば高速性を望むのであれば、後述の実施例のようにこれら鍵依存初期線形変換部302、鍵依存最終線形変換部308、鍵依存線形変換部353については、そのいずれか、もしくはすべてを省略することが可能である。この場合、差分解読法及び線形解読法に対する安全性は低下しない一方で、削除した分だけ暗号化処理速度の向上が望める。ただし他の解読法に対しては弱くなるおそれはある。また、鍵依存初期線形変換部302、鍵依存最終線形変換部308、鍵依存線形変換部347, 353のいずれか、もしくはすべてを鍵に依存しない線形変換部に変更することも可能である。この場合、差分解読法及び線形解読法以外の解読法に対しても安全性が低下しない一方で、インプリメントを最適化することにより、暗号化処理速度の向上が望める。なお、線形変換部としては、ビット位置を予め決めた関係で入れかえる転置、予め決めたビット数だけ回転シフトするなどを行う。鍵依存線形変換部は、鍵データに応じたビット数だけ回転シフトする、あるいは、鍵データとの排他的論理和演算を行うものなどである。

実施例 2

図6は、図3の第1実施例の非線形関数部304（図4）における2段目の4つの非線形変換部348～351のうち、中央の2つを省略した実施例を示す。この実施例では更に、図3における鍵依存初期線形変換部302と鍵依存最終線形変換部308も省略している。

平文に相当する入力データPを入力部301から暗号装置内に入力する。入力データPは初期分割部303で2つのブロックデータ L_0 , R_0 に分割される。ブロックデータ R_0 は、鍵記憶部322に保持されている鍵データ k_{00} , k_{20} と共に第0段ラウンド処理部308の非線形関数部304に入力され、非線形関数部304で変換処理を受けて、データ Y_0 に変換される。データ Y_0 とデータ L_0 は線形演算部30

5 で演算され、データ L_0^* に変換される。データ L_0^* とデータ R_0 は交換部306 でデータ位置のスワップが行われ、 $L_1 = R_0$, $R_1 = L_0^*$ とされる。以下、第 i 段ラウンド処理部 38 _{i} ($i=1, \dots, n-1$) において2つのデータ L_i , R_i について上記と同様の処理を繰り返し行う。即ち、2つのデータ L_i , R_i について、データ R_i は、鍵記憶部322 に保持されている鍵データ k_{0i} , k_{2i} と共に非線形関数部304 に入力され、非線形関数部304 で変換処理を受けて、データ Y_i に変換される。データ Y_i とデータ L_i は線形演算部305 で演算され、データ L_i^* に変換される。データ L_i^* とデータ R_i は交換部306 でデータ位置の交換が行われ、 $L_{i+1} = R_i$, $R_{i+1} = L_i^*$ のように変換される。

暗号方式としての安全性を確保するための適切な繰り返し回数を n とすると、 n ラウンドの繰り返し処理の結果、データ L_n , R_n が得られる。このデータ L_n , R_n を最終結合部307 で結合した後、出力部309 から暗号文として出力データ C を出力する。

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文 C から平文 P が得られる。

図7Aは、図6の実施例における第 i 段ラウンド処理部 38 _{i} の非線形関数部304 の機能構成を示す。前段からの入力データ R_i は、鍵記憶部322 に保持されている鍵データ k_{0i} , k_{2i} と共に非線形関数部304 への入力データとなる。データ R_i は、鍵依存線形変換341 において、データ k_{0i} によりデータ R_i^* に線形変換される。次に、データ R_i^* は分割部342 において4つのデータ in_0 , in_1 , in_2 , in_3 に分割される。4つのデータ in_0 , in_1 , in_2 , in_3 は、それぞれ非線形変換部343, 344, 345, 346において、データ mid_{00} , mid_{01} , mid_{02} , mid_{03} に非線形変換された後、線形変換部354 に入力される。線形変換部354 では、例えば図7Bに示すように4つの処理系列 30₀ ~ 30₃ 間でデータ相互に関連づけるように変換される。これは図5中の鍵データとの論理演算を省略した場合と同じ例であり、下記の式で表わせる。

$$mid_{10} = mid_{00} \oplus mid_{02} \oplus mid_{03}$$

$$mid_{11} = mid_{02} \oplus mid_{03}$$

$$mid_{12} = mid_{00} \oplus mid_{01} \oplus mid_{02} \oplus mid_{03}$$

$$\text{mid}_{13} = \text{mid}_{00} \oplus \text{mid}_{01} \oplus \text{mid}_{02} \quad (12)$$

この線形変換で、均質化されたデータ mid_{10} , mid_{11} , mid_{12} , mid_{13} が生成され、そのうちのデータ mid_{10} , mid_{13} は、それぞれ非線形変換部348, 351において、データ out_0 , out_3 に非線形変換された後、結合部352 において、4つのデータ out_0 , mid_{11} , mid_{12} , out_3 が1つのデータ Y_i^* に結合される。最後に、データ Y_i^* は、データ k_{2i} による鍵依存線形変換部353 において、データ Y_i に線形変換され、非線形関数部304 からの出力データ Y_i が生成される。

非線形変換部343～346は4つ並列に配置されており、その変換処理は相互に関連していないため、これらは並列実行が可能である。また、非線形変換部348, 351についても同様のことがいえる。この実施例では、各非線形関数部304 内の2段目の非線形変換部が外側の2つ (348, 351) だけに減らされているため、それだけ暗号化又は復号化処理量を削減することができる。

なお、鍵データ k_i は、鍵入力部320 から暗号装置内に入力された鍵情報 Key から鍵データ生成部321 によって変換され、鍵記憶部322 に保持されたデータである。

上記のように構成された暗号装置の場合、例えば、非線形変換部343～346, 348, 351が差分解読法及び線形解読法に対して確率 $p_b = 2^{-6}$ で近似表現できるように設計されているならば、実施例1と同様に各ラウンドは確率 $p_i \leq 2^{-12}$ で近似表現することができ、暗号装置全体としてはラウンド数 n を $n=3m$ として、確率 $p \leq 2^{-24m}$ で近似表現できることになる。ここで、例えば $m=4$ (ラウンド数12段) とすると、 $P \leq 2^{-96}$ となり、差分解読法及び線形解読法に対して十分安全な暗号装置となる。

また、鍵依存線形変換部353 があるため、差分解読法と線形解読法以外の解読法に対しても安全性にマージンがある構造であり、かつ実施例1よりも構造が簡素化されているため、処理量が軽減されている。つまり、安全性と低処理量のバランスを重視した暗号装置である。

実施例3

図8は、図6の第2実施例の非線形関数部304 において鍵依存線形変換部353 を省略した実施例を示す。平文に相当する入力データ P を入力部301 から暗号装

置内に入力する。入力データ P は初期分割部 303 で 2 つのブロックデータ L_0 , R_0 に分割される。ブロックデータ R_0 は、鍵記憶部 322 に保持されている鍵データ k_0 と共に第 0 段ラウンド処理部 380 の非線形関数部 304 に入力され、非線形関数部 304 で変換処理を受けて、データ Y_0 に変換される。データ Y_0 とデータ L_0 は線形演算部 305 で演算され、データ L_0^* に変換される。データ L_0^* とデータ R_0 は交換部 306 でデータ位置の交換が行われ、 $L_1 = R_0$, $R_1 = L_0^*$ のように変換される。以下、第 i 段ラウンド処理部 38 $_i$ では、2 つの入力ブロックデータ L_i , R_i について上記と同様の処理を繰り返し行う。即ち、2 つのデータ L_i , R_i について、データ R_i は、鍵記憶部 322 に保持されている鍵データ k_i と共に非線形関数部 304 に入力され、非線形関数部 304 で変換処理を受けて、データ Y_i に変換される。データ Y_i とデータ L_i は線形演算部 305 で演算され、データ L_i^* に変換される。データ L_i^* とデータ R_i は交換部 306 でデータ位置の交換が行われ、 $L_{i+1} = R_i$, $R_{i+1} = L_i^*$ とされ、ブロックデータ L_{i+1} , R_{i+1} が出力される。

暗号方式としての安全性を確保するための適切な繰り返し回数を n とすると、繰り返し処理の結果、データ L_n , R_n が得られる。このデータ L_n , R_n を最終結合部 307 で結合した後、出力部 309 から暗号文として出力データ C を出力する。

復号については、暗号化処理手順と逆の手順をたどることによって、暗号文 C から平文 P が得られる。

図 9 は、図 8 の実施例における非線形関数部 304 の機能構成を示す。非線形関数部 304 への入力データ R_i は、鍵記憶部 322 に保持されている鍵データ k_i と共に鍵依存線形変換 341 への入力となる。データ R_i は、鍵依存線形変換 341 において、鍵データ k_i によりデータ R_i^* に線形変換される。次に、データ R_i^* は分割部 342 において 4 つのデータ in_0 , in_1 , in_2 , in_3 に分割される。4 つのデータ in_0 , in_1 , in_2 , in_3 は、それぞれ非線形変換部 343, 344, 345, 346 において、データ mid_{00} , mid_{01} , mid_{02} , mid_{03} に非線形変換された後、線形変換部 354 に入力される。線形変換部 354 では、例えば実施例 2 の図 7 B と同じように、

$$mid_{10} = mid_{00} \oplus mid_{02} \oplus mid_{03}$$

$$mid_{11} = mid_{02} \oplus mid_{03}$$

$$mid_{12} = mid_{00} \oplus mid_{01} \oplus mid_{02} \oplus mid_{03}$$

$$\text{mid}_{13} = \text{mid}_{00} \oplus \text{mid}_{01} \oplus \text{mid}_{02} \quad (13)$$

に線形変換し、データ mid_{10} , mid_{11} , mid_{12} , mid_{13} を生成する。ついで、データ mid_{10} , mid_{13} は、それぞれ非線形変換部348, 351において、データ out_0 , out_3 に非線形変換された後、結合部352 において、4つのデータ out_0 , mid_{11} , mid_{12} , out_3 が1つのデータに結合され、非線形関数部304 からの出力データ Y_1 が生成される。

非線形変換部343～346は4つ並列に配置されており、その変換処理は相互に関連していないため、これらは並列実行が可能である。また、非線形変換部348, 351についても同様のことがいえる。

なお、鍵データ k_1 は、鍵入力部320 から暗号装置内に入力された鍵情報Key から鍵データ生成部321 によって変換され、鍵記憶部322 に保持されたデータである。

上記のように構成された暗号装置の場合、例えば、非線形変換部343～346, 348, 351が差分解読法及び線形解読法に対して確率 $p_b = 2^{-6}$ で近似表現できるように設計されているならば、各ラウンドは確率 $p_1 \leq 2^{-12}$ で近似表現することができ、暗号装置全体としてはラウンド数 n を $n=3m$ として、確率 $P \leq 2^{-24m}$ で近似表現できることになる。ここで、例えば $m=4$ (ラウンド数12段) とすると、 $P \leq 2^{-96}$ となり、差分解読法及び線形解読法に対して十分安全な暗号装置となる。

また、差分解読法及び線形解読法に対して十分な安全性を確保するために最低限必要な部しか実行しない構造であるため、処理量が軽減されており、かつ暗号化又は復号化速度もそれだけ改善されている。

上述において、非線形関数部304 中の各分割部342 は4分割に限らず、任意の複数に分割してもよい。なお、4分割の場合においては、第2の非線形変換部は図7A及び図9に示したように2つのみとすることができる。

上述した第2及び第3実施例で示した非線形関数部304 (ラウンド関数) における非線形変換部が6個 (343～346, 348, 351) の場合について、1ラウンド段当たりの安全強度と、安全性条件を満たすラウンド段数と、それに必要な処理量 (ステップ数) を図1及び図2に示したDES暗号装置の場合と比較して次の表に示す。ただし、この発明の実施例ではDESのS-box に対応する非線形変換部34

3 ～346 への入力データの全ビット数を32とし、従って、各非線形変換部への入力データは8ビットとしたため、これとサイズを合わせるため、DESの各S-boxのサイズを8ビットとし、従ってS-boxの数を4個として比較した。

比較表

	1段当たりの S-box 数	1段当たりの 安全性強度	必要な段数	ステップ数
DES	4	2^{-6}	17	68
この発明	6	2^{-12}	9	54

この表からわかるように、1段当たりのS-boxの個数（非線形変換部の数）が、この発明の方がDESより多いにもかかわらず、この発明の1ラウンド段当たりの安全性強度はDESの2倍となっている。そのため安全性条件を満たすためのラウンド段数はDESの場合より少なくなっており、またその安全性に必要な処理量（ステップ数）も少なくなっている。

発明の効果

以上、詳細に説明したように、この発明によれば、非線形関数部で入力データを複数に分割し、かつそれぞれ非線形変換を行い、その後、相互に線形交換を行い、更に少くとも一部を非線形変換することによりデータの通信または保持においてデータを秘匿するための暗号装置について、安全性が高い暗号装置を提供することができる。

請求の範囲

1. 鍵データを使って非線形変換を行う複数段のラウンド処理により入力データを順次処理して暗号化する暗号化装置であり、
入力データを2つのブロックデータに分割する初期分割部と、

鍵データを保持する鍵記憶部と、

上記2つのブロックデータが入力され、上記鍵データを使い順次処理を行う縦続接続された複数段のラウンド処理部と、

縦続接続された上記複数のラウンド処理部の最終段から出力される2つのブロックデータを1つのデータに結合し、その結合データを出力する最終結合部と、
を含み、

各段の上記ラウンド処理部は：

前段から入力された2つのブロックデータ的一方に対し、上記鍵記憶部に保持された鍵データに依存したデータ変換処理を行う非線形関数部と、

上記非線形関数部の出力データと、入力された上記2つのブロックデータの他方とを線形演算する線形演算部と、

上記線形演算部の出力データと上記非線形関数部への入力ブロックデータとを交換し、交換された2つのデータを次段の上記ラウンド処理部に2つの入力ブロックデータとして与える交換部と、

を含み、

上記非線形関数部は：

入力されたデータに上記鍵記憶部に保持された鍵データに基づいて線形変換を行い、変換データを生成する鍵依存線形変換部と、

上記鍵依存線形変換部からの変換データを複数個のビット列に分割する分割部と、

これらのビット列をそれぞれ非線形変換して変換データを出力する複数の第1非線形変換部と、

上記複数の第1非線形変換部からの変換データ間で線形変換を行い、均質化された複数のデータを複数の系列にそれぞれ出力する第1の線形変換部と、

上記複数の系列の少なくとも1つに設けられ、対応する上記第1線形変換部からの上記均質化されたデータに非線形変換を行い、変換データをその系列のデータとして出力する第2の非線形変換部と、

上記複数の系列からのデータを結合して上記非線形関数部の出力データとする結合部と、
を含む。

2. 請求項1に記載の暗号装置において、上記第1の線形変換部は、上記均質化された複数のデータを上記鍵記憶部に保持された鍵データに基づいて線形変換し、上記複数の系列のデータとして出力する鍵依存線形演算部を含む。

3. 請求項1又は2に記載の暗号装置において、上記結合部の出力データを線形変換して上記非線形関数部の出力データとする第2の線形変換部が設けられている。

4. 請求項3に記載の暗号装置において、上記第2の線形変換部は、上記鍵記憶部に保持された鍵データに基づいて線形変換を行う線形変換部である。

5. 請求項4に記載の暗号装置において、上記第1線形変換部は、各上記系列に少なくとも1つ設けられ、その系列のデータと他の系列のデータとの排他的論理和演算により上記均質化されたデータをその系列に出力する排他的論理和を含む。

6. 請求項1乃至5のいずれかに記載の暗号装置において、上記入力データに線形変換を行って上記初期分割部へ供給する初期線形変換部が設けられている。

7. 請求項6に記載の暗号装置において、上記初期線形変換部は上記鍵記憶部に保持された鍵データに基づいて線形変換を行う変換部である。

8. 請求項1乃至7のいずれかに記載の暗号装置において、上記最終結合部の出力データに線形変換を行って暗号装置の出力とする最終線形変換部が設けられている。

9. 請求項8に記載の暗号装置において、上記最終線形変換部は上記鍵記憶部に保持された鍵データに基づいて線形変換を行う変換部である。

10. 請求項1乃至9のいずれかに記載の暗号装置において、上記複数の系列は第1、第2、第3及び第4系列の順に次配列された4系列である。

11. 請求項10に記載の暗号装置において、上記第2非線形変換部は上記4つ

の系列のそれぞれに設けられている。

1 2. 請求項 1 0 に記載の暗号装置において、上記第 2 非線形変換部は上記第 1 及び第 4 系列にそれぞれ設けられている。

1 3. 請求項 1 2 に記載の暗号装置において、上記第 1 線形変換部は：

上記第 2 系列に設けられ、上記第 1 系列のデータと第 2 系列のデータの排他的論理和を演算する第 1 排他的論理和と、

上記第 3 系列に設けられ、上記第 4 系列のデータと第 3 系列のデータの排他的論理和を演算する第 2 排他的論理和と、

上記第 3 系列に設けられ、上記第 2 排他的論理和の出力と上記第 1 排他的論理和の出力との排他的論理和を演算する第 3 排他的論理和と、

上記第 2 系列に設けられ、上記第 1 排他的論理和の出力と上記第 3 排他的論理和の出力との排他的論理和を演算する第 4 排他的論理和と、

上記第 1 系列に設けられ、上記第 1 系列のデータと上記第 4 排他的論理和の出力との排他的論理和を演算する第 5 排他的論理和と、

上記第 4 系列に設けられ、上記第 4 系列のデータと上記第 3 排他的論理和の出力との排他的論理和を演算する第 6 排他的論理和と、
を含む。

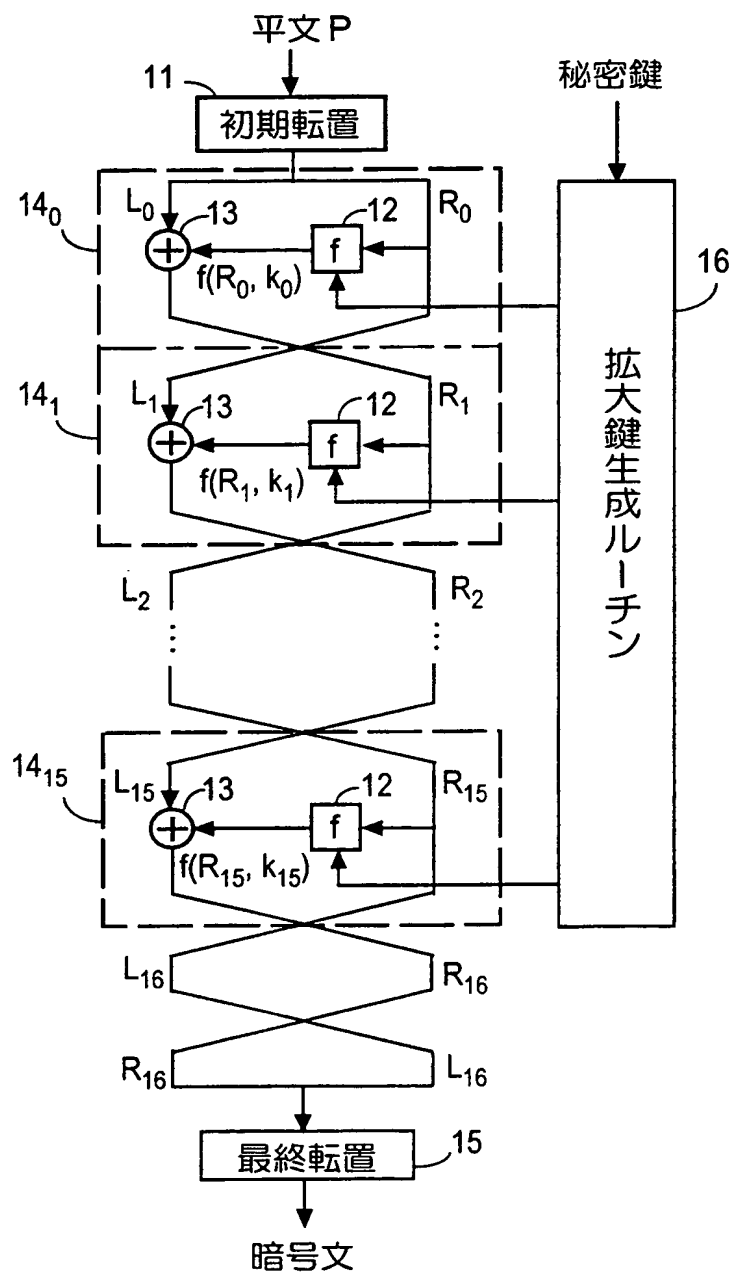


図 1

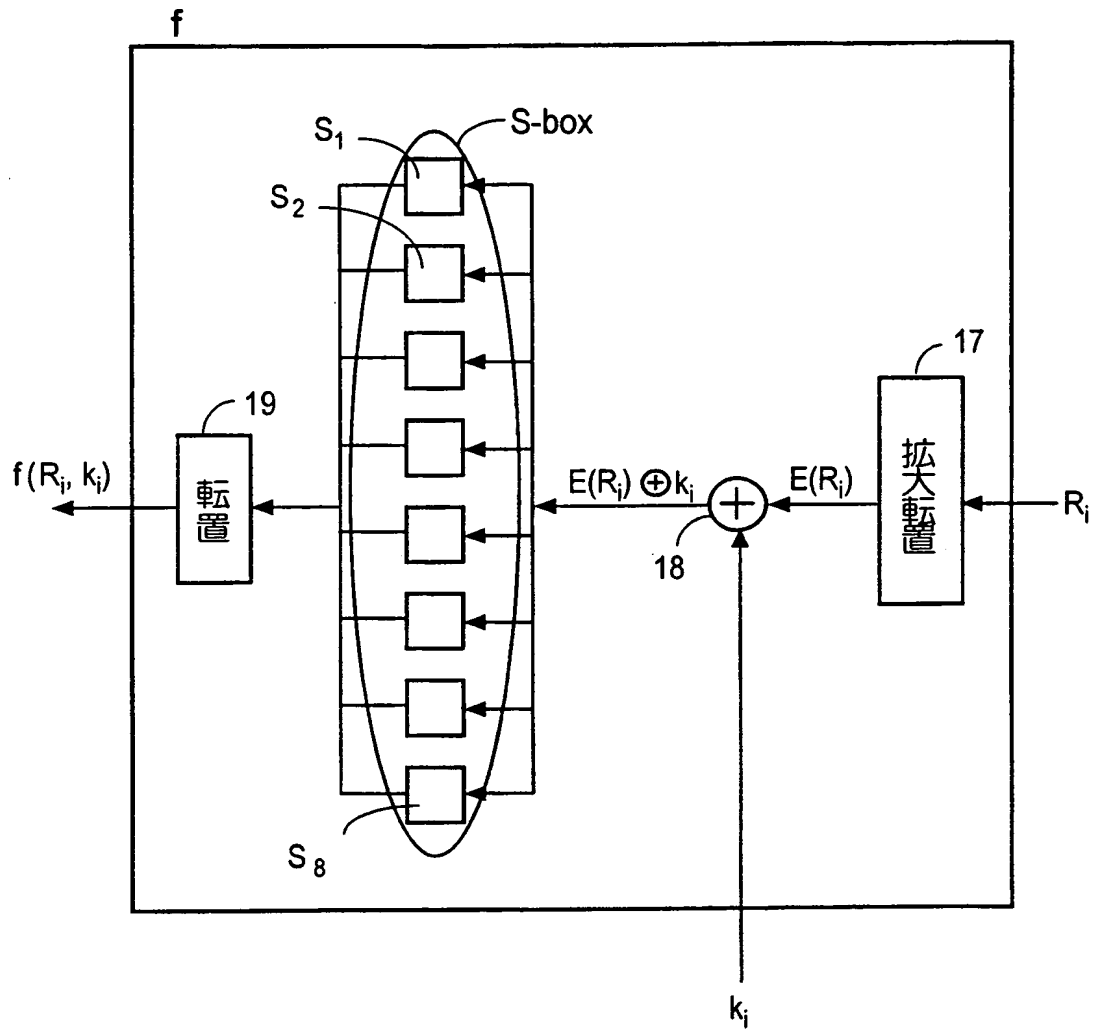


図 2

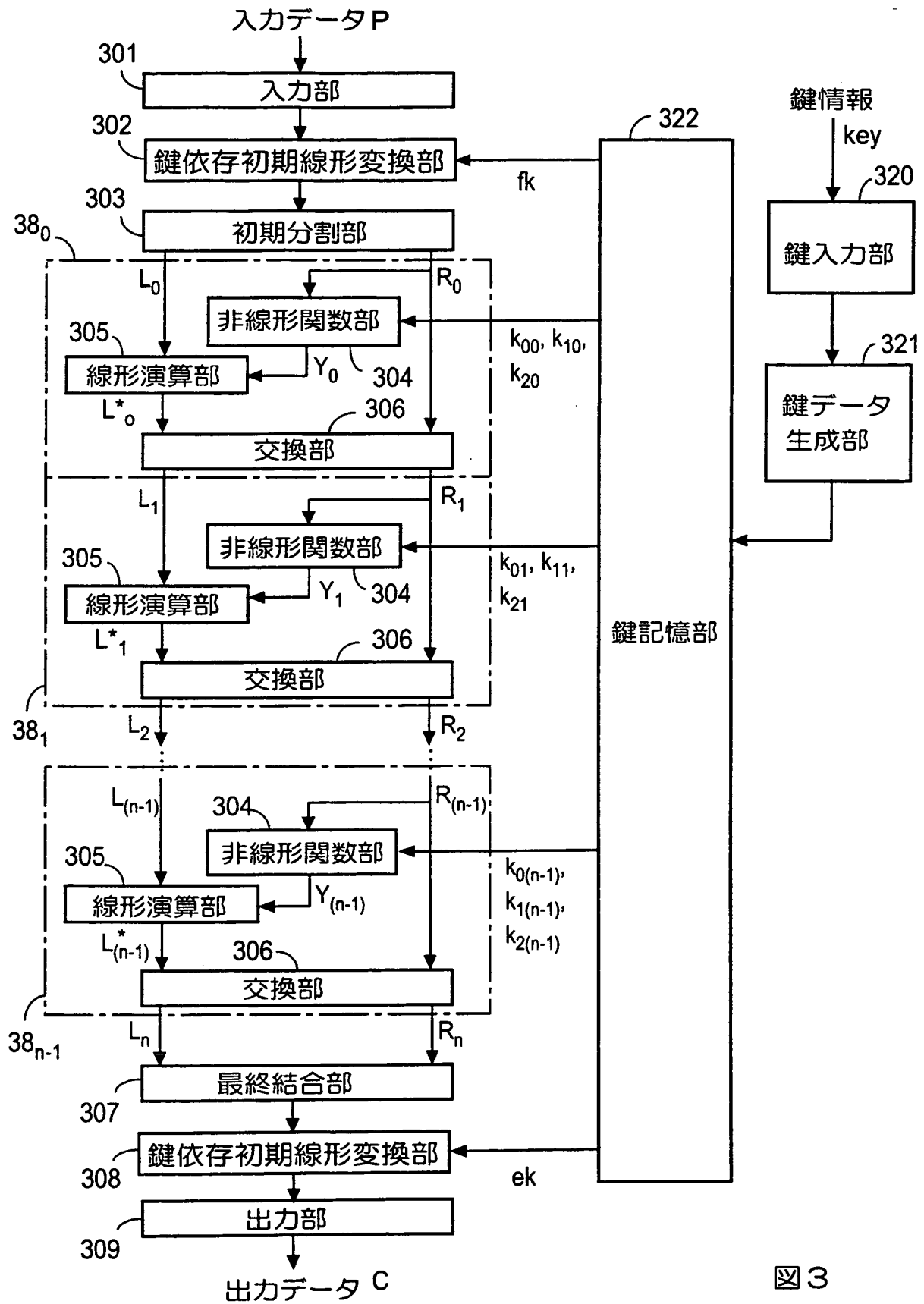
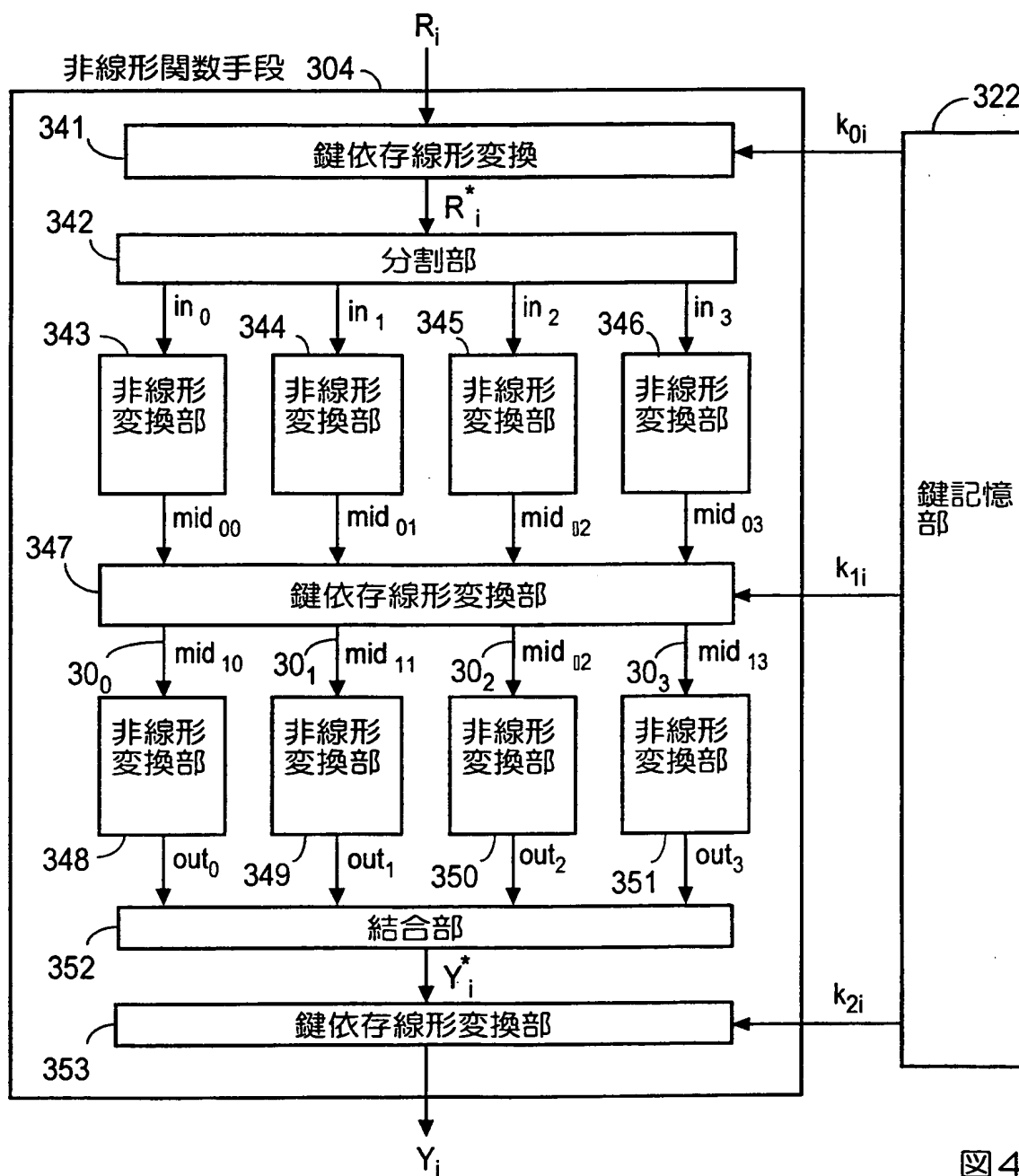


図 3





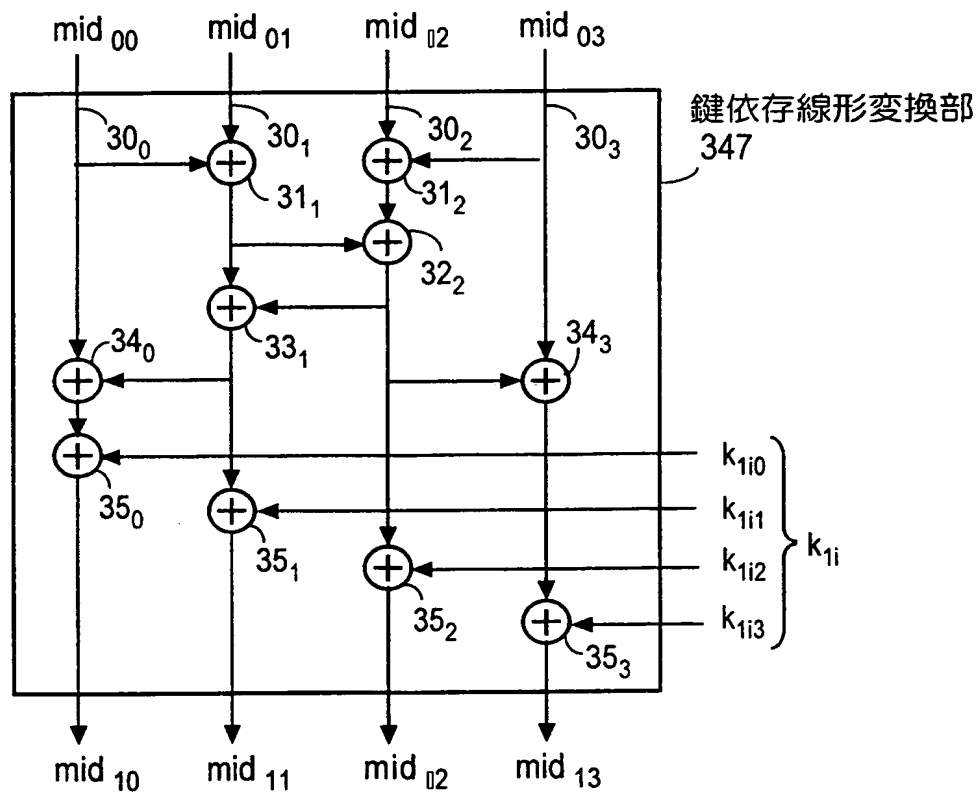


図 5

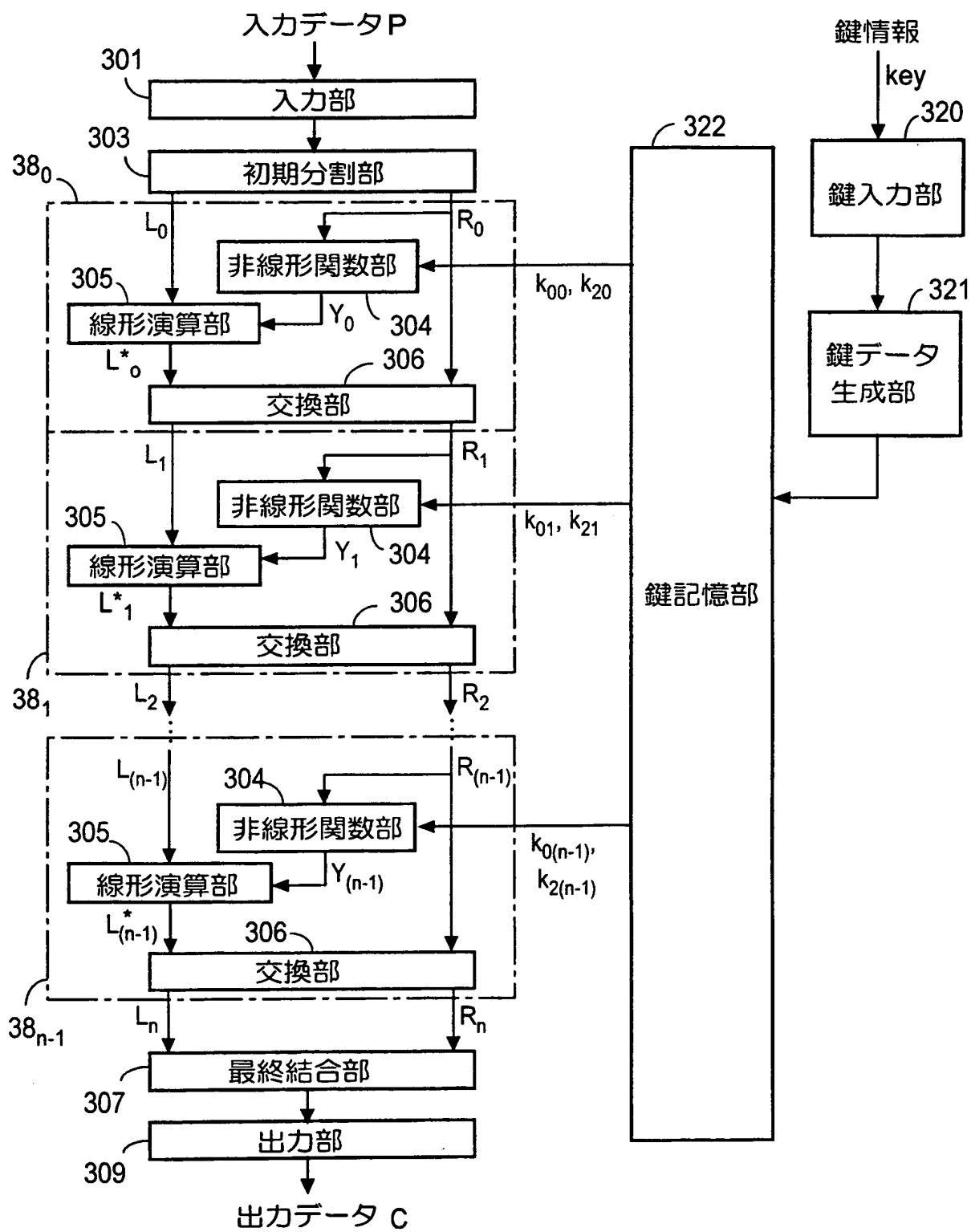


図 6

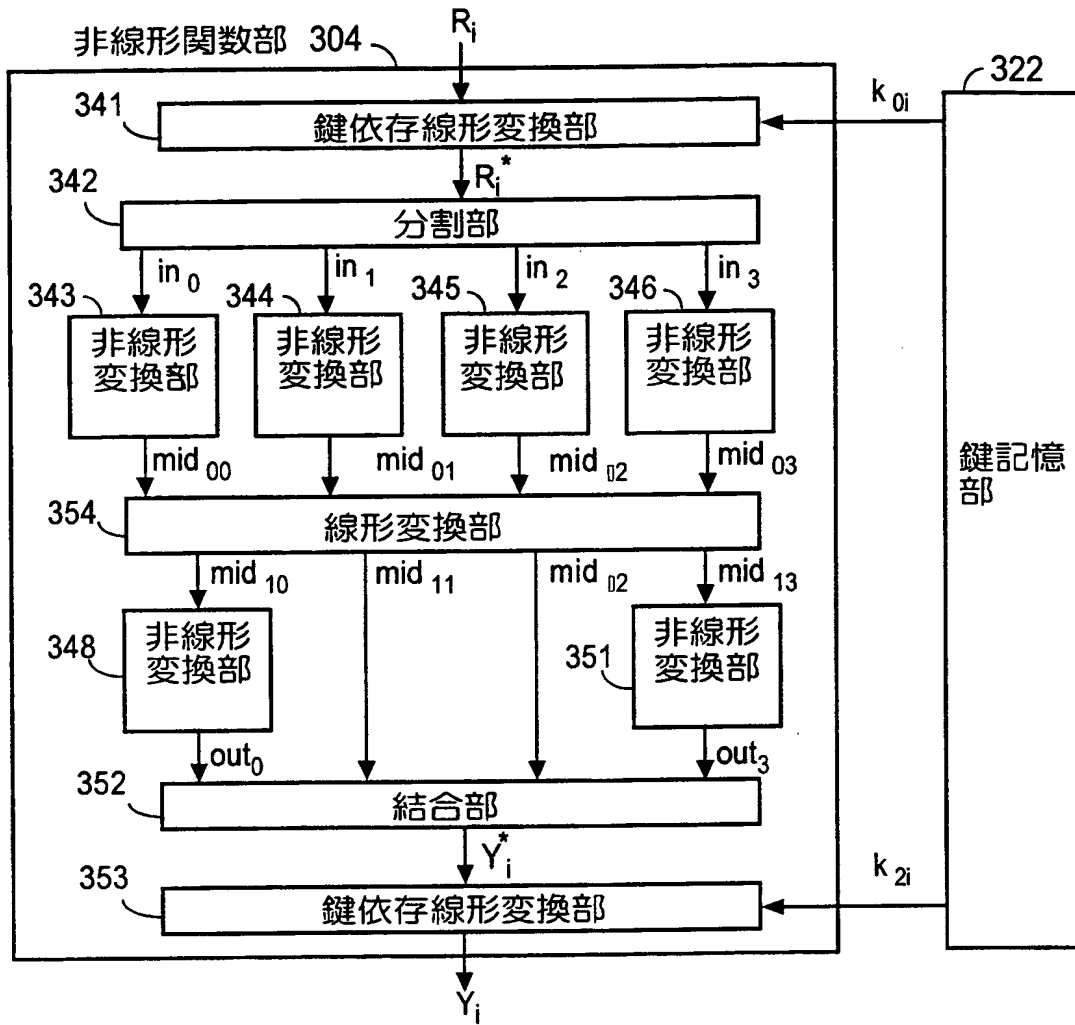


図7A

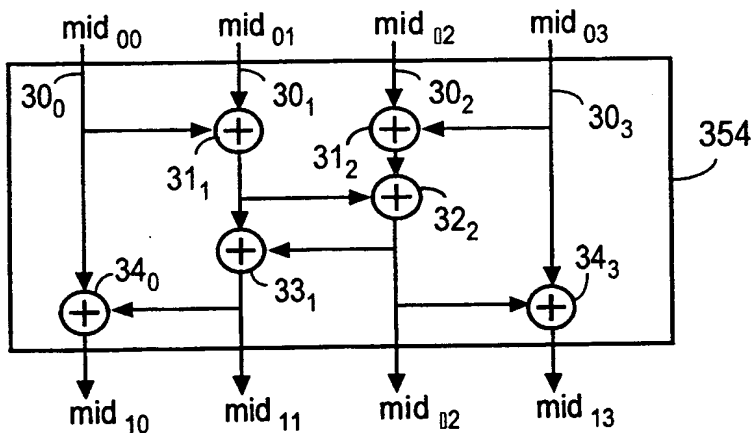


図7B

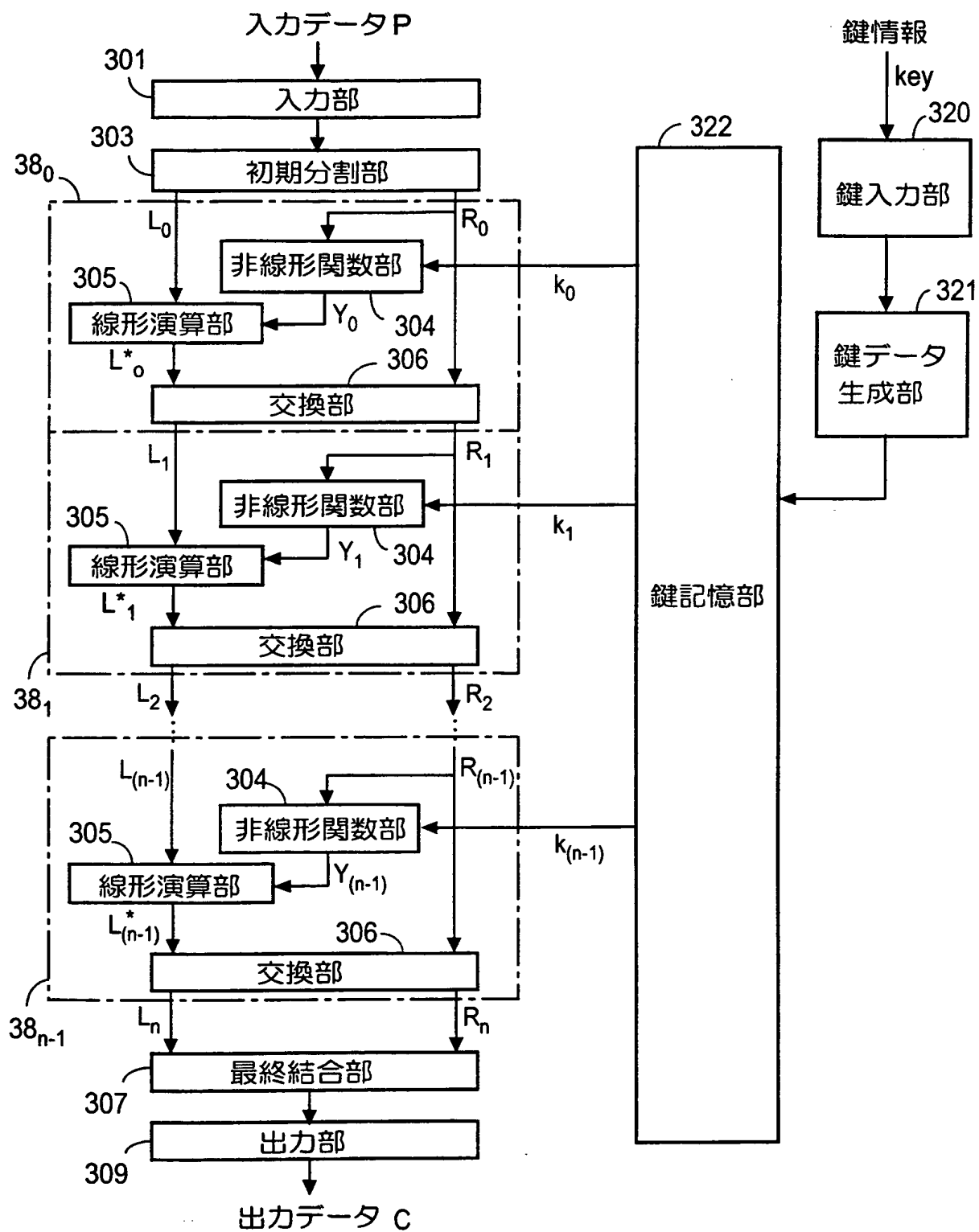


図 8

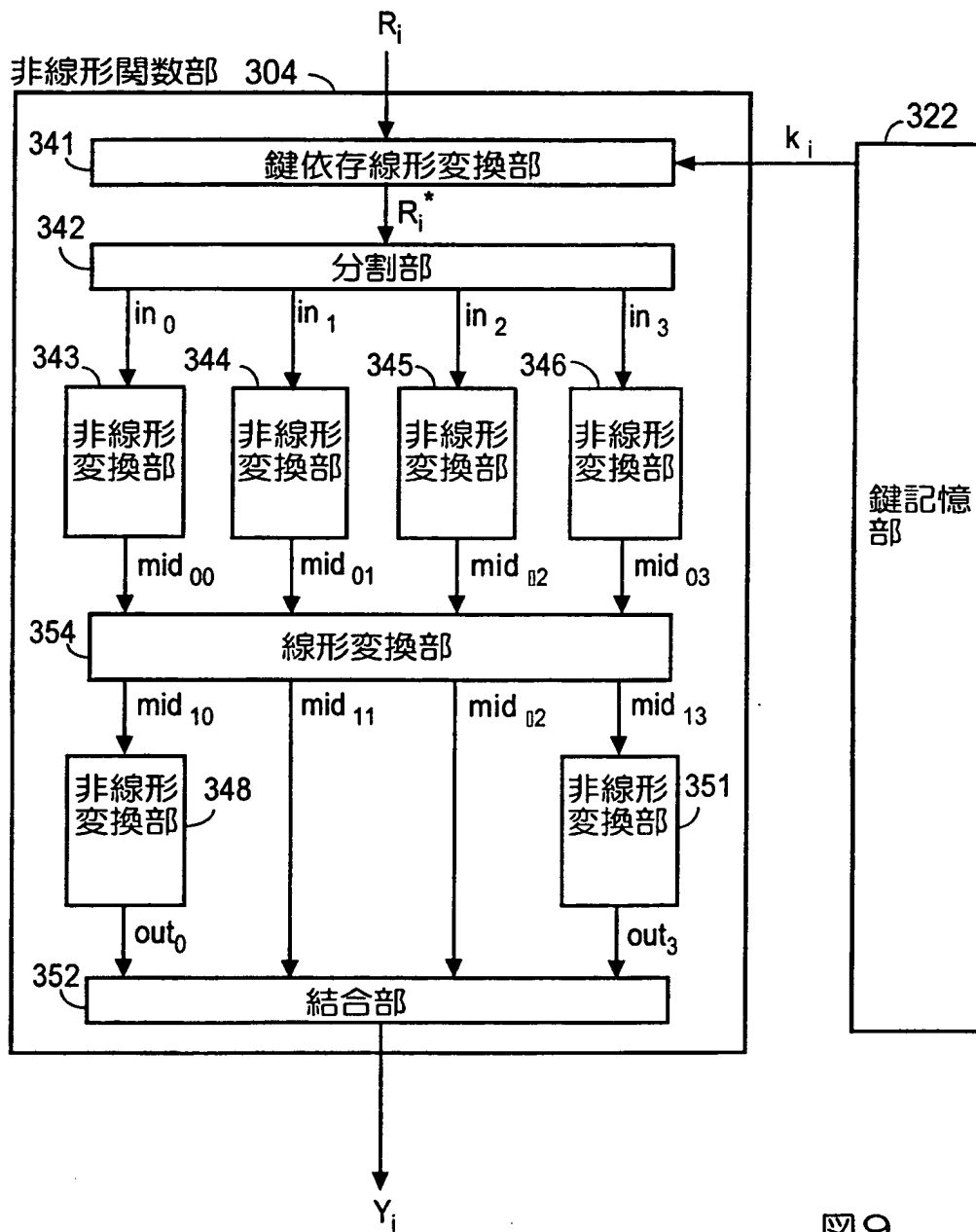


図 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP98/02915

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁶ G09C1/00, H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁶ G09C1/00, H04L9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1998
Kokai Jitsuyo Shinan Koho 1971-1998 Jitsuyo Shinan Toroku Koho 1996-1998

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO, 98/09705, A1 (Mitsubishi Electric Corp.), 13 March, 1997 (13. 03. 97), Full text ; Figs. 1 to 29 & AU, 6629396, A1 & NO, 972052, A & EP, 790595, A1	1-13
A	Mitsuru Matsui, "Provable Safety of Differential Decoding and Linear Decoding of Block Cipher (in Japanese)", Preprint of the 18th Symposium on Information Theories and their Applications, The Institute of Information Theories and their Applications, Vol. 1 of 2 October 1995 (10. 95) p.175-178	1-13
A	Mitsuru Matsui, et al., "Practical Block Cipher Having Provable Safety of Differential Decoding and Linear Decoding (in Japanese)", Symposium on Cipher and Information Security, SCIS96, Information Security Research Special Committee of IEICE, January 1996 (01. 96) SCIS96-4C	1-13

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
17 September, 1998 (17. 09. 98)

Date of mailing of the international search report
29 September, 1998 (29. 09. 98)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/02915

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 9-54547, A (NEC Corp.), 25 February, 1997 (25. 02. 97), Full text ; Figs. 1 to 11 (Family: none)	1-13
P, A	Masato Kanda, et al., "Structure of Round Function Using a Little S-box (Part 1) (in Japanese)", Technical Research Report of IEICE (ISEC97 14-22), Vol. 97, No. 181, 18 July, 1997 (18. 07. 97) p.41-52	1-13

国際調査報告

国際出願番号 PCT/J P 98/02915

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁶ G09C1/00, H04L9/06

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁶ G09C1/00, H04L9/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-1998年
 日本国登録実用新案公報 1994-1998年
 日本国実用新案登録公報 1996-1998年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	WO, 98/09705, A1 (三菱電機株式会社) 13. 3月. 1997 (13. 03. 97) 全文, 第1-29図 & AU, 6629396, A1 & NO, 972052, A & EP, 790595, A1	1-13
A	松井充, ブロック暗号の差分解読法と線形解読法に対する証明可能安全性について, 第18回情報理論とその応用シンポジウム予稿集, 情報理論とその応用学会, Vol. 1 of 2 10月. 1995 (10. 95) p. 175-178	1-13

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」先行文献ではあるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」同一パテントファミリー文献

国際調査を完了した日

17. 09. 98

国際調査報告の発送日

29.09.98

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5 J

4 2 2 9

印

電話番号 03-3581-1101 内線 3538

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	松井充 他, 差分解読法と線形解読法に対する証明可能安全性をもつ実用ブロック暗号, 暗号と情報セキュリティシンポジウムASCIS96講演論文集, 電子情報通信学会情報セキュリティ研究専門委員会, 1月. 1996 (01. 96) SCIS96-4C	1-13
A	JP, 9-54547, A (日本電気株式会社) 25. 2月. 1997 (25. 02. 97) 全文, 第1-11図 (ファミリーなし)	1-13
P, A	神田雅透 他, 少数のS-boxを用いたラウンド関数の構成について(その1), 電子情報通信学会技術研究報告 (ISEC97 14-22), Vol. 97, No. 181, 18. 7月. 1997 (18. 07. 97) p. 41-52	1-13